Functional Safety and Reliability Reference Flow for Automotive Applications

Cadence

ABSTRACT

ADAS (Advanced Driver Assistance System) applications are driving new trends and demands on car electronic systems. The myriad of sensors around the car are collecting a large data volume to be processed and transferred at high speed. This sets the demand for high performance compute platforms which can only be achieved using advanced nodes, such as TSMC 16FFC. High-speed communication channels are also a necessity and functional safety requires the use of deterministic protocols, such as Time Sensitive Networking.

Safety-critical applications for automotive have stringent requirements for Functional Safety and Reliability. Traditionally these requirements and expertise have been developed on older nodes, while now these needs to be migrated to advanced nodes. EDA methodologies and IPs for ADAS applications, in a joint effort with the foundry, can increase productivity when combining Functional Safety and Reliability requirements with advanced nodes support.

This presentation will cover the Functional Safety and Reliability methodologies for automotive applications, and some of the capabilities will be demonstrated on the Giga Ethernet MAC IP that has been ASIL-B certified. The Ethernet MAC also supports the Time Sensitive Networking protocol used in safety critical designs and can be deployed in sensor networks in ADAS applications.

The ISO26262 standard for automotive functional safety comprises new requirements during the design and verification flow to address systematic and random errors and meet the desired ASIL level. The presentation will focus on the flow support for design techniques (such as redundancy and BIST) to achieve the desired metrics. Simulation capabilities to verify the required levels of Diagnostic Coverage will also be discussed.

Automotive applications also add special requirements for reliability due to longer lifetime (10-15 years). Temperature exacerbates these effects and needs to be modeled properly. The signoff flow will be discussed to model failure mechanisms such as ESD and EM, including self-heating effects.

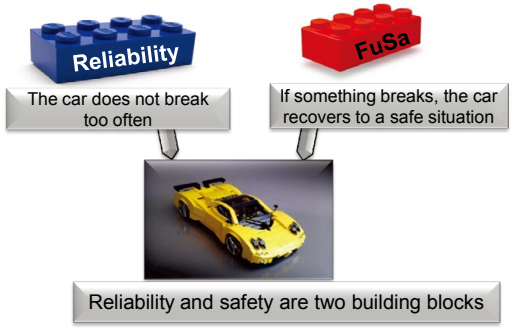
Functional Safety and Reliability Reference Flow for Automotive Applications

Alessandra Nardi, Software Engineering Group Director
TSMC OIP
San Jose, California
September 2016

cadence

Automotive Requirements

- Safety critical applications have stringent requirements on
  - Functional Safety
  - Reliability
- In the past
  - Limited amount of electronics
  - Older nodes

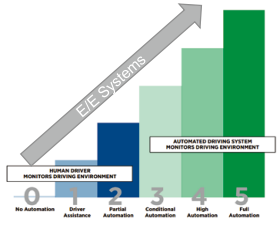


cadence

Automotive Requirements: What Changes?

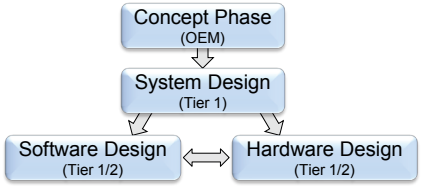
- Safety critical applications have stringent requirements on
  - Functional Safety
  - Reliability
- Advanced driver assistance systems (ADAS) are changing the game

Amount of electronics is growing fast (with the level of autonomous driving)



Source: http://www.sae.org/misc/pdfs/automated_driving.pdf

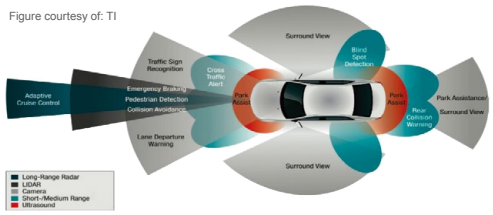
Complexity is increasing
- Divide and conquer
- Requirements are rippling down the chain



cadence

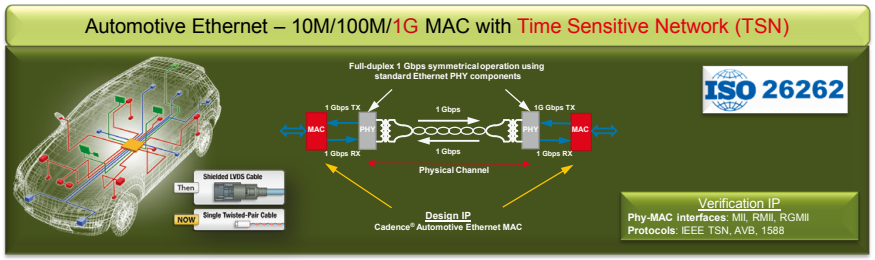
ADAS Bring New Opportunities and Challenges

Figure courtesy of: TI



High Performance and Flexible Compute Platform

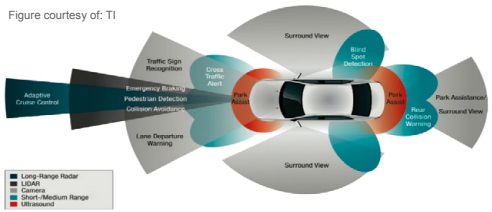
High-Speed Communication



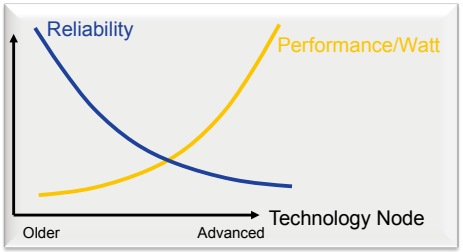
cadence

ADAS Bring New Opportunities and Challenges

Figure courtesy of: TI



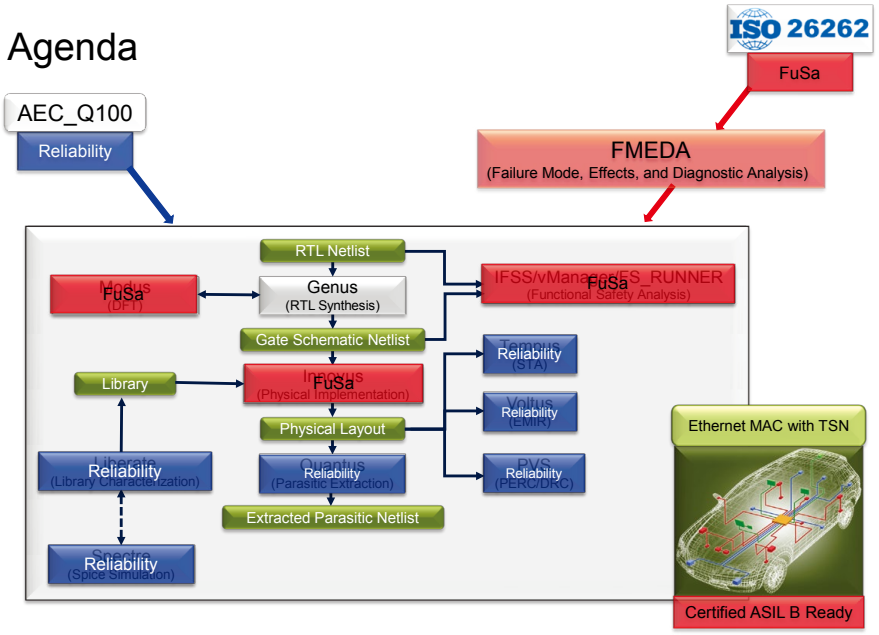
- High Performance and Flexible Compute Platform
- High-Speed Communication
- Advanced Nodes Support/Ecosystem



- High Compute Power can only be achieved with advanced nodes
- Reliability is more challenging on advanced nodes
- Migration effort from older nodes to be managed
- Collaboration between foundry and EDA is key for productivity

cadence

Agenda



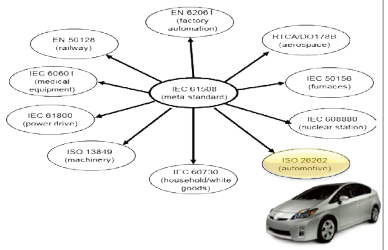
cadence

cadence

ISO 26262—Functional Safety Principles

Covers random and systematic errors

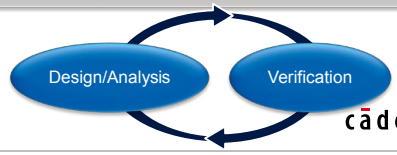
ISO 26262 defines
- Processes to follow
- Hardware/software performance to achieve
- Safety documentation to produce
- Software tools compliance process



Systematic Failures (e.g., software bug)	Random Failures (e.g., component malfunction, noise injection)
• Addressed by processes (planning, traceability, documentation, specs, …) • Strictness of processes are dependent on the ASIL level	• Includes permanent failure and transient effects • Addressed by design and inclusion of safety mechanisms to correct/detect faults (e.g. ECC) • Demonstrated by calculations of reliability/verification of failure rates • Failure rates and diagnostic coverage requirement depend on ASIL

FuSa Management

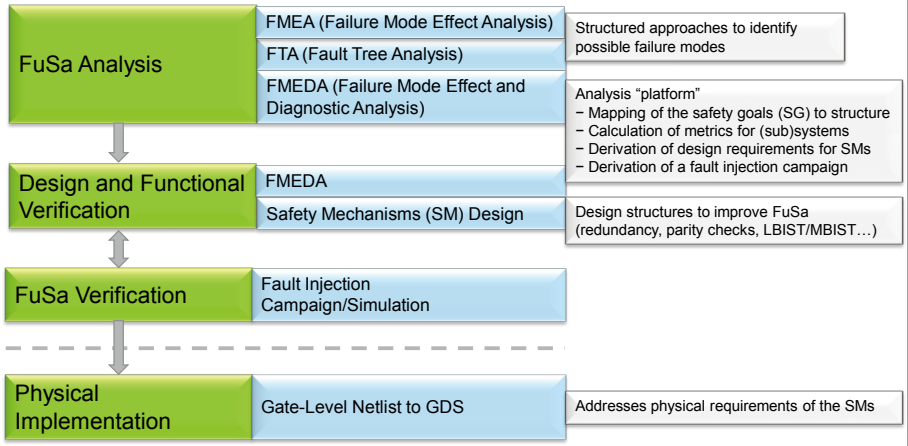
Tools ISO Compliance



cadence

Functional Safety (FuSa) Flow

Abstract semiconductor view

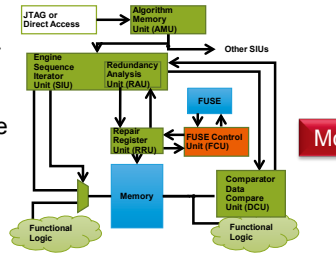


cadence

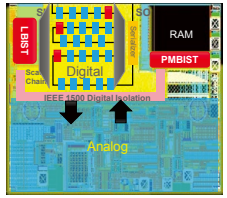
Safety Mechanisms

Modus Memory BIST, Logic BIST to meet the coverage needs

- IEEE 1500
  - Digital logic isolation from analog
  - Isolate blocks for in-system LBIST
- Test point analysis/insertion
  - Achieve ISO 26262/ASIL coverage goals
  - Minimize design impact and overhead
- Logic BIST
  - Area efficient
  - Use for POR or in-system testing
- Memory BIST
  - Built-in redundancy analysis and self repair
  - Programmable runtime algorithms
  - Use for POR or in-system testing
- Advanced fault modeling
  - Exhaustive, bridging fault, cell aware



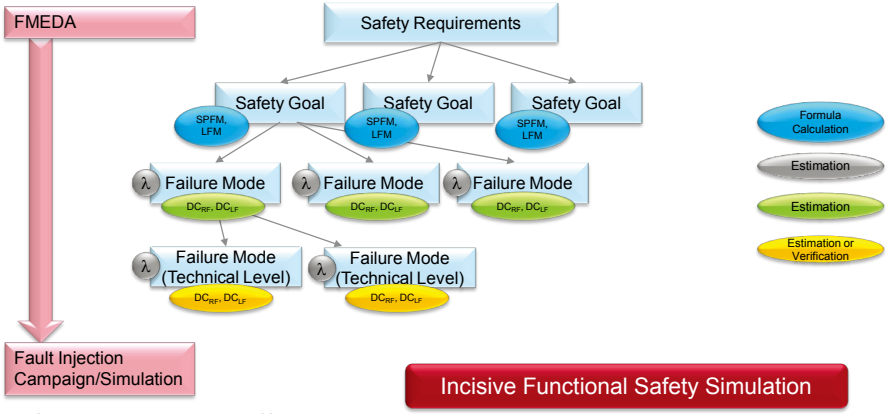
Modus™ Test



cadence

FuSa Analysis to FuSa Verification

FMEDA to fault injection campaign/simulation



- Statistical, intelligent generation of faults related to safety goals
- Fault simulation
- Fault classification and diagnostic coverage

Incisive Functional Safety Simulation

ASIL metrics:
- SPFM (Single Point Fault Metric)
- LFM (Latent Fault Metric)
- DCRF (Residual Fault Diagnostic Coverage)
- DCLF (Latent Fault Diagnostic Coverage)
- λ Failure Rate

cadence

Physical Implementation (of the SM)

Innovus Functional Safety and High Reliability design

- Safety mechanisms are used to improve FuSa by increasing the diagnostic coverage (ability to detect a failure and bring the system into a safe state)
- Redundancy only helps when there is true independence of the redundant logic
- Physical Implementation needs to support true independence by avoiding common cause failures

Table D.4 — Processing units

Safety mechanism/measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Self-test by software: limited number of patterns (one channel)	D.2.3.1	Medium	Depends on the quality of the self test
Software diversified redundancy (one hardware channel)	D.2.3.4	High	Depends on the quality of the diversification. Common mode failures can reduce diagnostic coverage
HW redundancy (e.g. Dual Core Lockstep, asymmetric redundancy, coded processing)	D.2.3.6	High	It depends on the quality of redundancy. Common mode failures can reduce diagnostic coverage

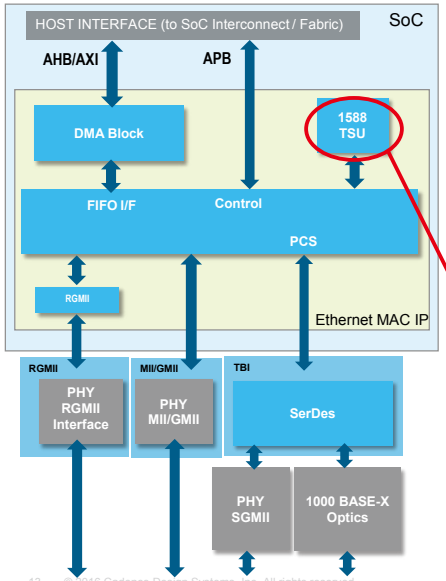
Excerpt from ISO 26262-5:2011(E) – Annex D (Evaluation of Diagnostic Coverage)

- Placement, routes, and vias
  - Same value register spacing (multiple voting flops) – special placement
  - Logic isolation - safety islands
  - Power-domain routing - specific safety coloring
  - Reliability - 100% multi-cut via coverage

Innovus™ Implementation

cadence

10/100/1000M Automotive Ethernet MAC/PCS IP



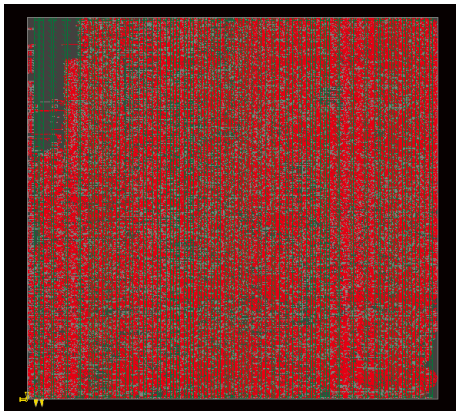
- Provides the logic required to integrate a Gigabit Ethernet MAC and 1000BASE-X PCS into any SoC
- Enables deterministic, real-time data transfer for safety-critical applications supporting the Time Sensitive Network Protocol (IEEE 802.1as / 1588)
- Certified as ASIL-B ready

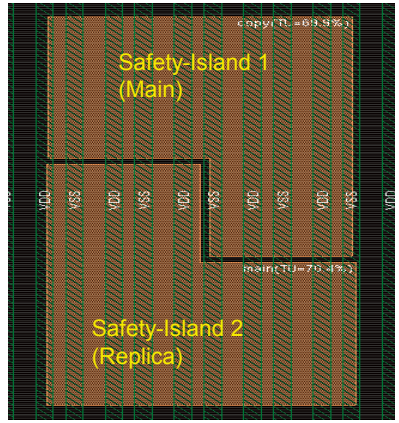
- Time Stamp Unit (TSU) is key to the TSN standard
- TSU output protection identified during FMEDA as key to improve Functional Safety
- TSU block duplicated and provided instant detection of faults (automatic comparison of each of the TSU's timer output, on a cycle-to-cycle basis)

cadence

Physical Implementation of the Ethernet MAC IP

Technology: TSMC 16 FFC TSMC





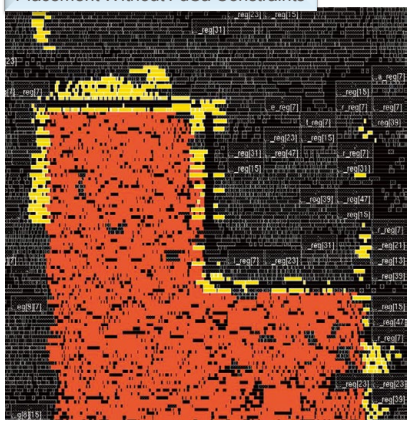
Instance Count: ~150K, Design Utilization ~ 70%

cadence

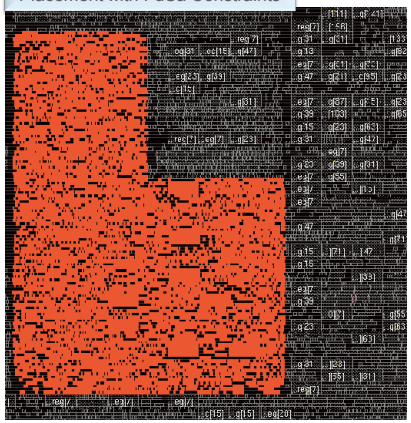
Placement to Support Module Independence

Cell spacing to avoid common cause failures

Placement Without FuSa Constraints



Placement with FuSa Constraints

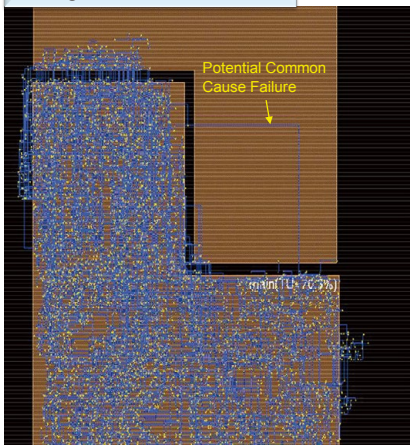


cadence

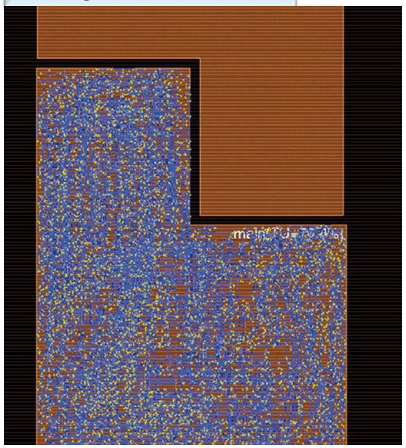
Routing to Support Module Independence

Wire routing to avoid common cause failures

Routing Without FuSa Constraints



Routing with FuSa Constraints

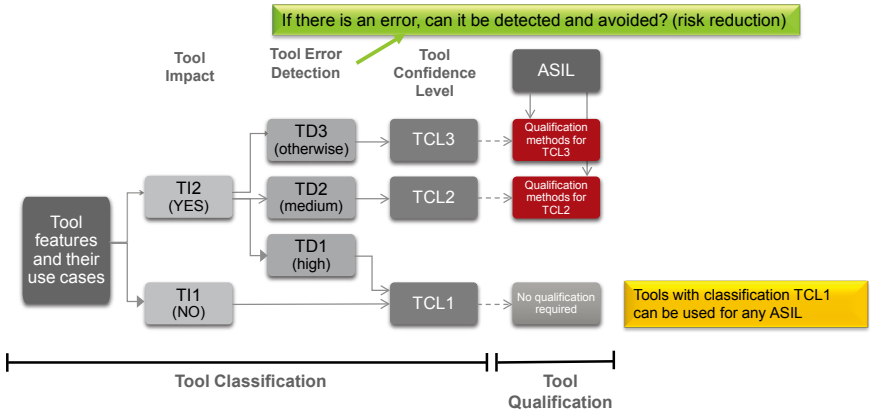


- Internal-nets should not leave safety island boundaries
- Interface-nets should not route over the other island
- The next level net after an interface-net (i.e., after a buffer) can cross the other island
- External wires (i.e., not belonging to either island) have no restrictions

cadence

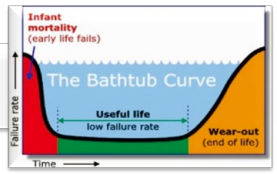
Tool Confidence Level (TCL)—ISO 26262:8

EDA tools are supporting processes in the FuSa design and verification flow



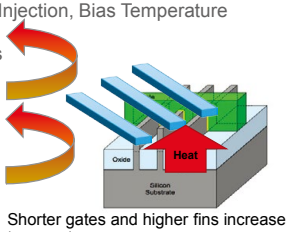
Automotive Reliability Challenges

- Measured by the FIT (Failure in Time) rate
  - 1 FIT = 10^{-9} → 1 failure per billion hours (once in about 114,155 years)
  - Equivalently, MTBF (Mean Time Between Failure) = 1/FIT
- Function of time (equivalent hours)



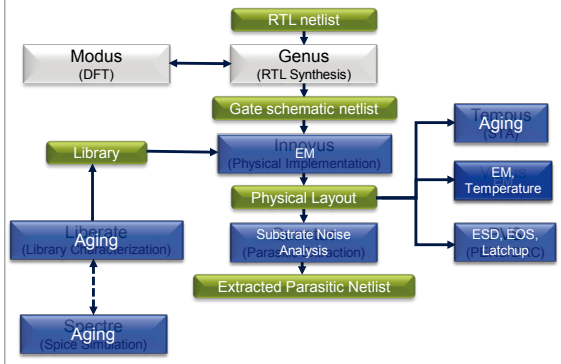
Electromigration
Aging
Latchup, ESD
Temperature

- Device lifetime expectation of 15-20 years
  - Aging: Transistor performance degraded over time by Hot Carrier Injection, Bias Temperature Instability, Time Dependent Dielectric Breakdown
  - EM: Interconnect shorts and opens created over time, voltage loss
- Powertrain direct mount, junction temperature of 175°C
  - Temperature: Impacts IC performance, accelerates aging and EM
- Now based on advanced nodes such as TSMC 16FFC
  - FinFET ICs: Significant self heating
- Actuators demand significant current and voltage
  - Power ICs: Significant current, voltage, temperature, and noise



- Shorter gates and higher fins increase temperatures
- More heat accumulation due to narrow fin structure and lower thermal connectivity

Reliability on the complete flow



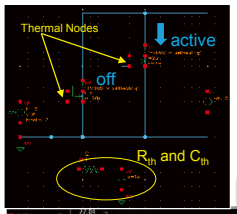
Automotive requirements:

- Aging: transistor performance degraded over time by Hot Carrier Injection, Bias Temperature Instability, and Time Dependent Dielectric Breakdown
- EMIR: Interconnect shorts and opens created over time, voltage loss
- Electrical Stress: ESD, EOS, Latchup
- Power ICs: significant current, voltage, temperature and noise
- Temperature: impacts IC performance, aging and EMIR
- Finfet ICs: significant self-heating

Tempus™
Innovus Implementation
Quantus™ QRC
Virtuoso® Electrically Aware Design
Voltus™/Voltus-Fi
Liberate™
Spectre®
PVS

Electro-Thermal Analysis and Simulation

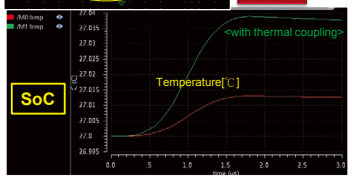
Temperature impacts performance, aging, and EM

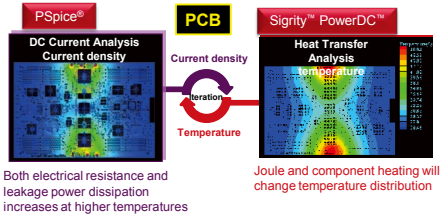


Custom simulation with high-temperature aging

Models supporting thermal analysis and thermal coupling:
HiCUM, BSIMSOI, HBT, HiSIM_HV

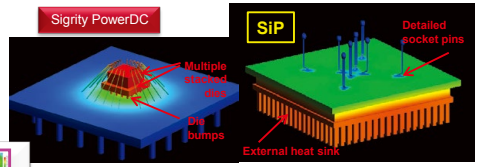
Spectre

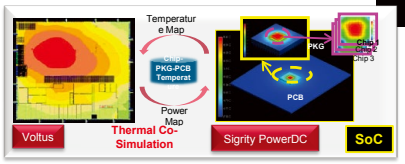




Both electrical resistance and leakage power dissipation increases at higher temperatures

Joule and component heating will change temperature distribution



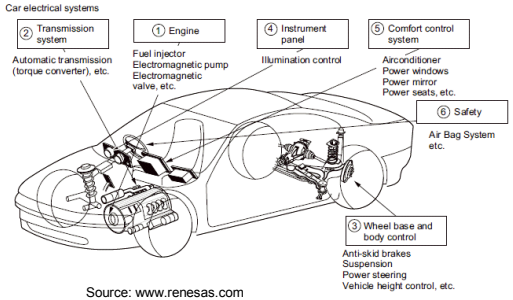


Detailed and accurate thermal solutions for each and every shape, trace, via, solder/bump, wire, lead, socket, etc.

cadence

Automotive PowerICs

- Electronic stability control, ADAS, and autonomous cars rely on actuators (control motors or solenoids) to control the vehicle
- Actuators demand significant current and voltage, managed by PowerICs created for these automotive applications
  - These can be a significant noise source through the substrate

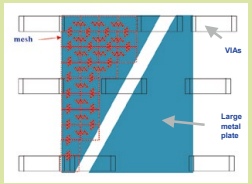


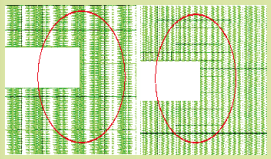
Source: www.renesas.com

cadence

PowerMOS Extraction

Adaptive Resistance Meshing



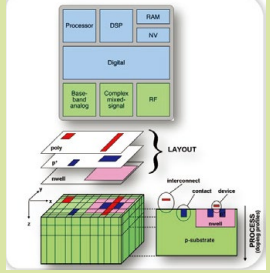


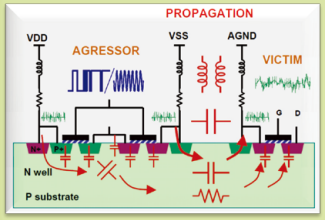
Uniform Meshing | Adaptive Meshing Around Irregular Features

- For large metal plates and vias
- Optimizes performance and accuracy
- Works well on irregular shapes and wide metal plates

Quantus QRC

Substrate Noise Analysis

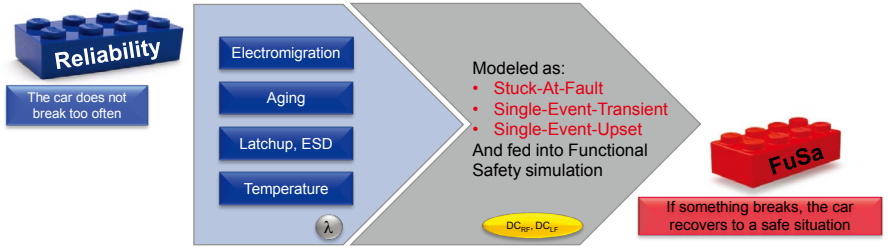


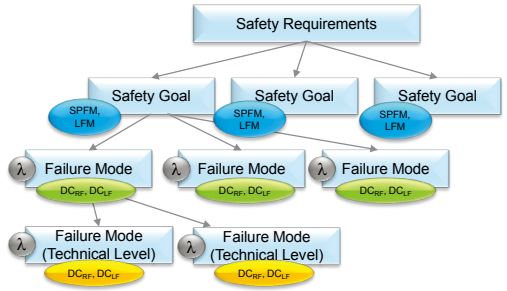


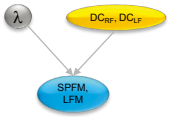
- Full 3D substrate model; accurate within ~7% of measurement data
- Provides isolation strategies (guardrings) to reduce noise in design

cadence

A View Back to Functional Safety



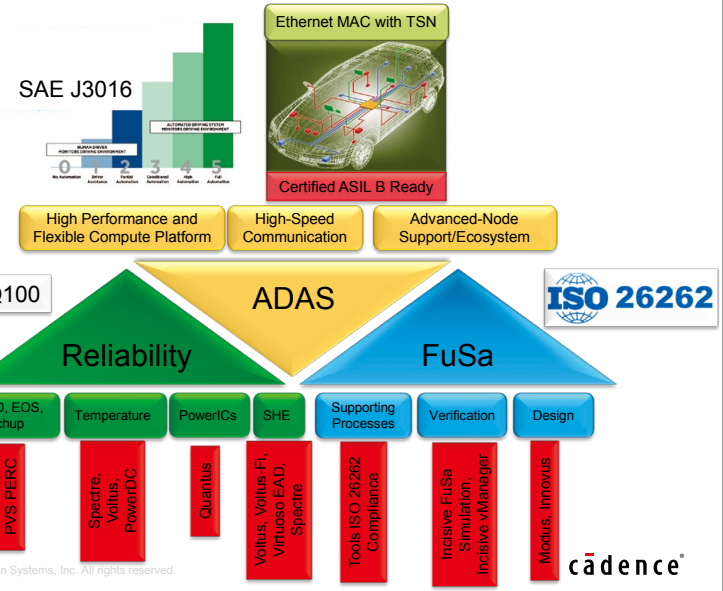




cadence

Automotive Requirements and Trends

ADAS complexity pushing more and more demands on E/E systems



cadence®